



What's New for FortiMail 5.2.0



What's New for FortiMail 5.2.0

September 2, 2014

1st Edition

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Fortinet Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

What's New	4
New VM platform support.....	4
New antispam features	5
Spam outbreak protection	5
Behavior analysis	6
Newsletter detection	6
Integration enhancement with FortiSandbox.....	6
LDAP group in ACL rules	6
URI exempt list	7
Digitally sign outbound email with S/MIME	7
MX record support in mail routing rules	8
LVM support on FortiMail VM	8
New server mode features.....	8
Email retention for sent email	9
Email address automatic completion in webmail	9
CardDAV support.....	9
Email filter in webmail	9
Favicon and webmail help customization.....	10
Content profile query on LDAP server	10

What's New

FortiMail 5.2.0 GA release is one of the FortiMail major releases, which comes with many new features and enhancements. This document lists the following ones:

- New VM platform support
- New antispam features
- Integration enhancement with FortiSandbox
- LDAP group in ACL rules
- URI exempt list
- Digitally sign outbound email with S/MIME
- MX record support in mail routing rules
- LVM support on FortiMail VM
- New server mode features
- Content profile query on LDAP server

New VM platform support

In addition to VMware VSphere Hypervisor ESX/ESXi virtual machines, FortiMail VM 5.2.0 can now be installed on Microsoft Hyper-V servers. For more information, see the FortiMail VM (Hyper-V) Install Guide on docs.fortinet.com.

New antispam features

A few new antispam techniques have been added to 5.2.0 release to combat spam. These features are in the antispam profile settings under *Profile > AntiSpam > AntiSpam*.

The screenshot shows the 'AntiSpam Profile' configuration window. The 'Scan Configurations' section is expanded, displaying a list of antispam features. Four features are highlighted with red circles: 'Spam outbreak protection', 'Behavior analysis', 'Newsletter', and 'URI filter phishing'. Each feature has a checkbox and an associated 'Action' dropdown menu, all currently set to 'Default--'. The 'URI filter' dropdown is set to 'phishing'. Below the 'Scan Configurations' section are 'Scan Conditions' and 'Other Settings' sections, and 'Create' and 'Cancel' buttons at the bottom.

Spam outbreak protection

When there is a spam outbreak, FortiGuard antispam service may need some time to update its database. In this case, FortiMail can hold the suspicious email for a short period of time before it query the FortiGuard server for the second time.

To configure how long FortiMail will hold email before query FortiGuard for the second time, use this CLI command (note that this can only be configured with the CLI command):

```
config system fortiguard antispam
    set outbreak-protection-period <minutes>
end
```

The default interval is 30 minutes.

Behavior analysis

To improve spam catch rate, FortiMail uses the text part and HTML part of the email body to analyze the similarity of uncertain email against those well-known spam messages which are received recently.

Newsletter detection

Although newsletters and other marketing campaigns are not spam, some users may find them annoying.

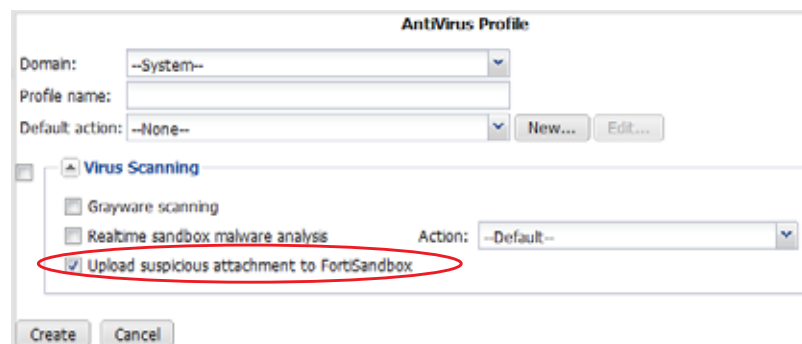
Enable detection of newsletters and select an action profile to deal with them. For example, you can tag newsletter email so that users can filter them in their email clients.

Integration enhancement with FortiSandbox

Integration with FortiSandbox has been enhanced to combat Advanced Persistent Threat (APT). Email is queued while suspicious files are sent to FortiSandbox for evaluation. After receiving query results from FortiSandbox, FortiMail will take actions that are defined in the relevant antivirus action profiles.

This feature is in the antivirus profile settings under *Profile > Antivirus > Antivirus*.

Figure 1: FortiSandbox integration



LDAP group in ACL rules

The user patterns now support LDAP groups under *Policy > Access Control > Receiving*.

Figure 2: LDAP group support in ACL

Access Control Rule

Enabled: ☒

Sender pattern: User Defined

Recipient pattern: Internal

Sender IP/netmask: LDAP Group

Reverse DNS pattern: *

Authentication status: Any

TLS profile: --None--

Action: REJECT

Comments:

Create Cancel

URI exempt list

In case a good URL is misconfigured and assigned to a spam category in the URI filter (under *Profile > AntiSpam > URI Filter*), you can correct the problem by specifying the URLs to be exempted from scanning and blocking.

To do this, go to *AntiSpam > URL Exempt List > Exempt*. The patterns can contain wild cards or regular expressions.

Figure 3: URL exempt list

URL Exempt

Exempt pattern: *

Pattern type: Default

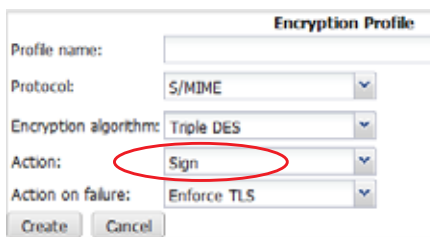
Create Cancel

Digitally sign outbound email with S/MIME

In addition to encryption, FortiMail can now sign the outgoing email with S/MIME.

This feature is added under *Profile > Encryption > Security > Encryption and Encryption > S/MIME > Certificate Binding*. When you configure an access control delivery policy, you can use the encryption profile.

Figure 4: Sign action in encryption profile



Encryption Profile

Profile name:

Protocol: S/MIME

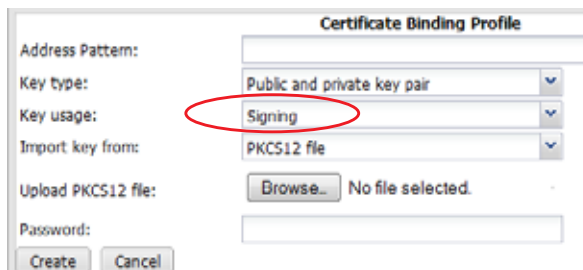
Encryption algorithm: Triple DES

Action: **Sign**

Action on failure: Enforce TLS

Create Cancel

Figure 5: Sign action in certificate binding



Certificate Binding Profile

Address Pattern:

Key type: Public and private key pair

Key usage: **Signing**

Import key from: PKCS12 file

Upload PKCS12 file: No file selected.

Password:

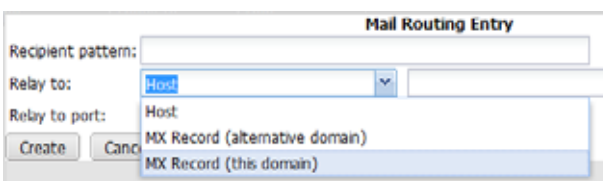
Create Cancel

MX record support in mail routing rules

The mail routing under *Profile > Session > Mail Routing* is part of the advanced MTA control features. By default, this feature is hidden. To enable it, use the following CLI command:

```
config system global
    set mta-adv-ctrl-status enable
end
```

Figure 6: MX record in mail routing



Mail Routing Entry

Recipient pattern:

Relay to: **MX Record (this domain)**

Relay to port:

Create Cancel

LVM support on FortiMail VM

The following CLI commands have been added to support the logical volume manager (LVM) on the FortiMail VM platforms.

```
execute lvm enable/disable
execute lvm extend
execute lvm summary
```

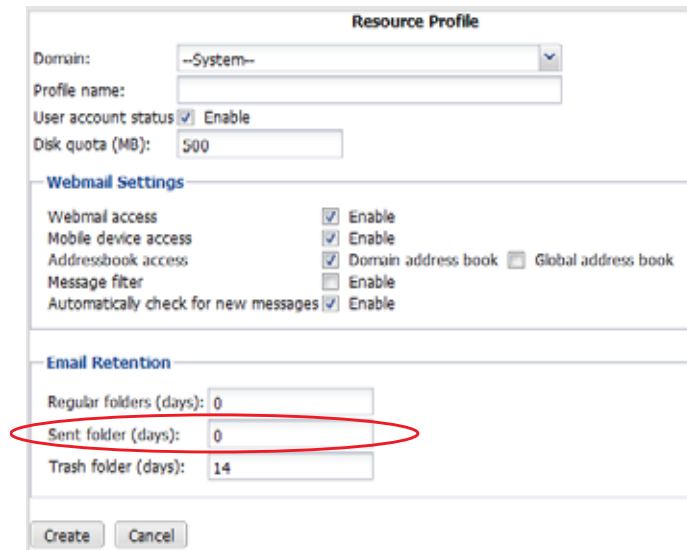
New server mode features

Several server mode features have been added to this release.

Email retention for sent email

Under *Profile > Resource Profile*, you can now configure the retention time for the sent email. The default value is 0, which means not to delete email.

Figure 7: Sent email retention



The screenshot shows the 'Resource Profile' configuration window. It includes fields for 'Domain' (set to '--System--'), 'Profile name', 'User account status' (checked 'Enable'), and 'Disk quota (MB)' (set to 500). Below these are 'Webmail Settings' with checkboxes for 'Webmail access', 'Mobile device access', 'Addressbook access', 'Message filter', and 'Automatically check for new messages', all of which are checked. Under 'Email Retention', there are three input fields: 'Regular folders (days)' set to 0, 'Sent folder (days)' set to 0 (highlighted with a red oval), and 'Trash folder (days)' set to 14. At the bottom are 'Create' and 'Cancel' buttons.

Email address automatic completion in webmail

When composing email in webmail, automatic address suggestions from the address book will be displayed while you are typing.

CardDAV support

In addition to WebDAV and CalDAV services, FortiMail now supports CardDAV calendar sharing service.

Email filter in webmail

In the resource profile settings under *Profile > Resource > Resource*, you can enable the message filter so that the webmail users will be able to set up filter rules under their preference settings. If not enabled, the webmail users will not be able to use this feature.

Figure 8: Message filter contro on admin GUI

The screenshot shows the 'Resource Profile' configuration page. Under the 'Webmail Settings' section, the 'Message filter' checkbox is checked and highlighted with a red circle. Other settings include 'Domain' set to '--System--', 'Profile name' as an empty field, 'User account status' checked, 'Disk quota (MB)' set to 500, 'Webmail access' checked, 'Mobile device access' checked, 'Addressbook access' checked, 'Domain address book' checked, 'Global address book' unchecked, and 'Automatically check for new messages' checked. The 'Email Retention' section shows 'Regular folders (days)' as 0, 'Sent folder (days)' as 0, and 'Trash folder (days)' as 14. 'Create' and 'Cancel' buttons are at the bottom.

Favicon and webmail help customization

Under *System > Customization > Appearance*, you can now upload your own favicon image.

You can also choose not to show the online help link in the webmail. This might be useful if you do not want to show the help contents provided by Fortinet.

Figure 9: Favicon and online help customization

The screenshot shows the 'New Appearance' configuration page. Under the 'Administration interface' section, the 'Product icon' field is highlighted with a red circle, showing a 'FortiMail VM' logo. Below it, the 'Top logo (460*36)' field also shows the 'FortiMail VM' logo. The 'Default language' is set to 'English'. Under the 'Webmail interface' section, the 'Show online help link' checkbox is checked and highlighted with a red circle. Other settings include 'Webmail login' as 'Login', 'Login user name hint' as 'address', 'Webmail theme' as 'Red Grey', 'Allow user to change theme' checked, 'Custom online help URL' as an empty field, and 'Webmail language' as 'English'.

Content profile query on LDAP server

In the LDAP profile settings under *Profile > LDAP*, you can now choose to retrieve the content profile from the LDAP server. Only antispam and antivirus profiles can be retrieved before.

Figure 10: Content profile query

Edit LDAP Profile

Profile name:

Server name/IP: Port:

Fallback server name/IP: Port:

Use secure connection: [Test LDAP Query...]

☒ **User Query Options**

☐ **Group Query Options**

☒ **User Authentication Options**

☒ **User Alias Options**

☐ **Mail Routing Options**

☐ **Scan Override Options**

AntiSpam attribute:

AntiVirus attribute:

Content attribute:

☐ **Address Mapping Options**

☐ **Domain Lookup Options**

☐ **Remote Access Override Options**

☐ **Advanced Options**

